AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

BANK SAFETY LOCKER SYSTEM WITH IMAGE IDENTIFICATION BY USING IOT

[1] G. Lakshmi Prasanna, [2] M. Poojitha, [3] M. Madhavan Chary, [4] Behu Lokesh Sahu, [5] M. Akshay Kumar

[1] *Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

[2,3,4,5] *B. Tech Student, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

ABSTRACT

Traditional bank locker systems depend primarily on physical keys, PINs, or mechanical token-based authentication, which can be lost, duplicated, or misused. This project proposes a secure, IoT-enabled safety locker system augmented with image-based identification to improve security, convenience, and auditability. Each locker access request is verified using face recognition (or image-based identity confirmation) captured by a camera at the locker kiosk; the image is matched against a pre-registered customer profile stored securely in the cloud. The IoT platform manages access logs, real-time alerts, remote monitoring, and role-based access control for bank staff. Combining image identification with traditional multi-factor authentication (card + PIN + image) strengthens security while providing administrators with a searchable audit trail. The system supports remote management, automated alerts for suspicious events, and an encrypted cloud-backed log for regulatory compliance.

Keywords: IoT, Bank Locker, Image Identification, Face Recognition, Biometric Authentication, Cloud Logging, Real-Time Monitoring, Access Control, Security Automation, Encryption.

I. INTRODUCTION

Bank safety lockers hold customers' most valuable physical assets; consequently, access control must be robust, auditable, and user-friendly. Conventional locker systems often rely on mechanical keys and manual identification at the branch, which can introduce security gaps such as forged credentials, lost keys, or human error during verification. In a modern banking environment, customers expect faster, safer and more accountable access mechanisms without compromising on regulatory requirements.

Advances in image processing and IoT make it possible to strengthen locker security by adding image-based identity verification into the access workflow. A camera installed at the locker kiosk captures a live image at the point of access; an on-device or cloud-based recognition engine matches the live capture to the customer's registered image. Coupled with a smart-card or digital token and optional PIN or biometric factor, image identification forms part of a multi-factor authentication system that significantly reduces the risk of unauthorized access.

The IoT layer enables real-time communication between locker hardware, the recognition service, and the bank's central monitoring system. It permits remote alerts (for example, if an access attempt fails repeatedly or matches an unauthorized profile), centralized logging for audits, and administrative actions such as temporarily locking a locker or generating access reports. This convergence of IoT, image identification, and secure cloud services delivers improved security, compliance, and customer convenience.

II. LITERATURE SURVEY

1. Dr. R. S. Mehra — "Biometric and Image-Based Authentication for Secure Access Control"

Dr. Mehra investigated combining image-based recognition with conventional authentication to enhance access security in controlled

environments. The work evaluated different facial recognition algorithms and their robustness to lighting and pose variation. The study recommended hybrid verification flows — for instance, combining card-based verification with image recognition — to lower false acceptance rates while maintaining usability.

Dr. Mehra also discussed operational considerations such as anti-spoofing measures, image liveness detection, and edge vs. cloud processing trade-offs. The paper emphasized the importance of liveness checks (e.g., blinking, movement analysis) to prevent the use of printed or replayed images. In addition, privacy-preserving design principles and encrypted storage of biometric templates were recommended to comply with data protection regulations.

Finally, the research highlighted that integrating image-based authentication into existing security workflows improves audit trails; reliably matched images linked to timestamped access logs make incident investigation and compliance reporting far easier.

2. Prof. A. K. Jain — "IoT for Secure Physical Infrastructure: Design and Best Practices"

Prof. Jain explored how IoT devices can be architected for critical infrastructure security, including banks and vaults. He outlined best practices for secure device provisioning, secure communication (TLS, mutual authentication), and hardware hardening for kiosk devices deployed in public-facing spaces. His recommendations emphasized fail-safe modes for devices when connectivity is lost.

His work also addressed system-level monitoring and anomaly detection through telemetry collected from IoT endpoints. He showed how centralized logging and analytics could detect abnormal access patterns or device tampering, enabling timely interventions. Prof. Jain stressed strict access controls on administrative interfaces and periodic firmware integrity checks to mitigate supply-chain and runtime attacks.

The study concluded that IoT can significantly enhance physical security only when integrated with strong cryptography, secure lifecycle management, and operational monitoring — a blueprint directly relevant to secure bank locker implementations.

3. Dr. L. Fernandez — "Cloud-based Authentication and Audit Logging for Financial Services"

Dr. Fernandez focused on cloud-driven identity solutions for financial institutions, discussing secure storage of identity attributes, access tokens, and audit trails. The paper argued for fine-grained role-based access control, immutable logging (e.g., append-only logs or blockchain-like tamper evidence), and rich reporting for compliance audits.

She evaluated architectures where sensitive biometric templates are not stored in plain form, recommending template hashing or irreversible transformations to reduce privacy risk. The work also covered latency and availability trade-offs for cloud-based vs. edge-based recognition services, suggesting hybrid approaches where quick decisions are made on the edge while full verification and long-term logging happen in the cloud.

A key takeaway was that auditability and non-repudiation are central to bank environments; provisioning full, timestamped, image-linked access logs simplifies regulatory reporting and fraud investigations.

4. Mr. P. R. Desai — "User Experience and Workflow Optimization in Secure Access Systems"

Mr. Desai researched how secure access systems can be designed for minimal friction while preserving high security. His work explored user flows that combine physical tokens (cards), short PIN codes, and quick image verification to balance speed and security in real-world settings like bank branches.

He emphasized ergonomics and kiosk placement, clear feedback messages (visual and audio), and robust fallback procedures (e.g., staff-assisted override with multi-party verification). Mr. Desai's studies also underlined training front-line staff to handle exception paths and to maintain user trust when biometric checks fail.

His conclusions support a multi-modal access strategy for safety lockers — one that prioritizes first-pass success and clear, secure fallback paths to avoid undue customer inconvenience.

5. Ms. N. Gupta — "Privacy and Legal Aspects of Biometric and Image Data in Banking"

Ms. Gupta analyzed regulatory and privacy considerations around storing and processing biometric and image data in the banking sector. She examined consent flows, data minimization strategies, and jurisdictional compliance requirements such as encryption, retention periods, and the right to erase or dispute personal data.

Her recommendations included storing only derived, non-recoverable biometric templates, encrypting data at rest and in transit, logging consent, and providing customers with clear terms for image capture and usage. Ms. Gupta also emphasized periodic privacy impact assessments and audit trails documenting who accessed biometric data and for what purpose.

Her work is critical to any bank locker system with image identification; it guides the legal and policy design necessary to maintain customer trust and regulatory compliance.

III. EXISTING SYSTEM

Current bank locker access typically involves physical keys, metal tokens, or card-and-PIN mechanisms, often with in-branch identity verification performed by bank staff. Access records are usually maintained as manual logs or simple digital records with limited linkage to verifiable identity artifacts like images. When disputes or suspicious events occur, reconstructing events often relies on paper logs, CCTV footage (if available), and staff recollection. These processes can be slow and may lack cryptographic integrity required for forensic investigation.

IV. PROPOSED SYSTEM

The proposed system integrates **image identification**, multi-factor authentication, and an IoT backbone to manage and secure bank lockbox access. Workflow: the customer presents a token (smart card or mobile token) at a secure locker kiosk; the kiosk requests a PIN (if enabled) and captures a live image. The image is checked for liveness and matched against the customer's registered image using an on-edge or cloud-based recognition service. When all authentication factors pass, the kiosk actuates the locker mechanism to permit access and simultaneously writes a tamper-evident, timestamped log to the cloud. Real-time alerts can be sent to bank security if the match fails, liveness checks detect spoofing, or suspicious behavior occurs. Administrative dashboards allow branch managers to review image-linked access logs and to temporarily disable lockers or require in-branch verification for flagged events.

V. SYSTEM ARCHITECTURE

1. Locker Kiosk (Edge Device)

- Secure enclosure containing: lock actuator (electromagnetic or motorized), local microcontroller (Raspberry Pi / industrial edge device), camera module, smart-card / NFC reader, keypad (optional), display & speaker, tamper sensors.
- Runs local software for capture, liveness detection, and immediate safety interlocks.

2. Edge Processing & Security

- Lightweight image preprocessing and liveness checks occur at the edge to minimize latency and reduce spoofing attempts (blink detection, challenge-response). Only minimal feature

templates (or encrypted descriptors) may be sent to cloud — raw images are retained only if policy permits. All storage on device uses hardware encryption.

3. Network & IoT Gateway

- Secure TLS channel (mutual authentication) between kiosks and cloud. MQTT or HTTPS APIs for telemetry, access requests, and command-and-control. Gateway also supports local offline modes: if cloud unreachable, kiosks enforce conservative policies (e.g., deny access or require manual staff override).

4. Cloud Backend

- Authentication service (matching engine), encrypted database for user profiles and templates, tamper-evident audit log (append-only with hash chaining or blockchain-backed ledger if required), alerting engine (SMS/email/push), and administrative dashboard. Role-based access controls restrict who can view images and logs.

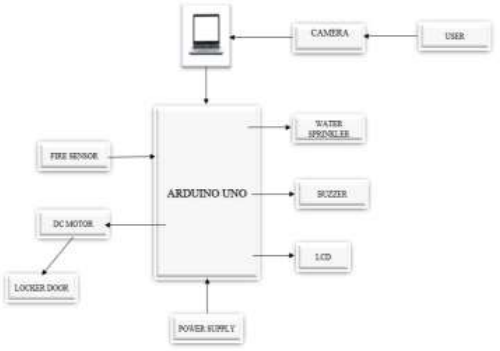

Fig.5.1: Structure of the working model

ARUDINO:

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmega microcontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/output pins, all on a single chip. Unlike, say, a Raspberry Pi, it's designed to attach all kinds of sensors, LEDs, small motors and speakers, servos, etc. directly to these pins, which can read in or output digital or analog voltages between 0 and 5 volts. The Arduino connects to your computer via USB, where you program it in a simple language (C/C++, similar to Java) from inside the free Arduino IDE by uploading your compiled code to the board. Once programmed, the Arduino can run with the USB link back to your computer, or stand-alone without it — no keyboard or screen needed, just power.

Starting clockwise from the top center:

- Analog Reference pin (orange)
- Digital Ground (light green)
- Digital Pins 2-13 (green)
- Digital Pins 0-1/Serial In/Out - TX/RX (dark green) - These pins cannot be used for digital i/o (Digital Read and Digital Write) if you are also using serial communication (e.g. Serial.begin).
- Reset Button - S1 (dark blue)
- In-circuit Serial Programmer (blue-green)
- Analog In Pins 0-5 (light blue)
- Power and Ground Pins (power: orange, grounds: light orange)
- External Power Supply In (9-12VDC) - X1 (pink)
- Toggles External Power and USB Power (place jumper on two pins closest to desired supply) - SV1 (purple)
- USB (used for uploading sketches to the board and for serial communication between the board and the computer; can be used to power the board) (yellow)

Received: 28-09-2025 | Accepted: 03-11-2025 | Published: 10-11-2025 | www.ajaccm.com

DIGITAL PINS

- In addition to the specific functions listed below, the digital pins on an Arduino board can be used for general purpose input and output via the pin Mode(), Digital Read(), and Digital Write() commands. Each pin has an internal pull-up resistor which can be turned on and off using digital Write() (w/ a value of HIGH or LOW, respectively) when the pin is configured as an input. The maximum current per pin is 40mA.

ANALOG PINS

In addition to the specific functions listed below, the analog input pins support 10-bit analog-to-digital conversion (ADC) using the analog Read() function. Most of the analog inputs can also be used as digital pins: analog input 0 as digital pin 14 through analog input 5 as digital pin 19. Analog inputs 6 and 7 (present on the Mini and BT) cannot be used as digital pins.

VI. IMPLEMENTATION

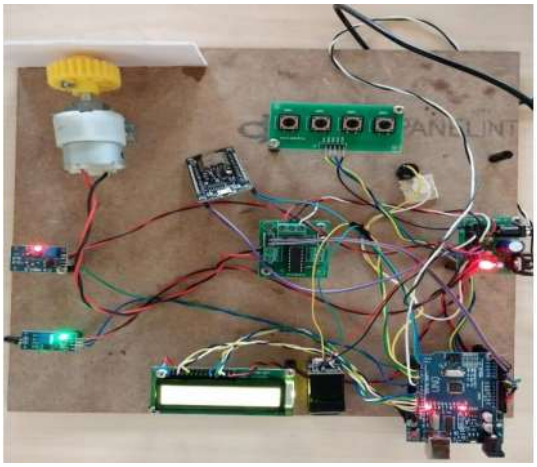

Fig. 6.1: Prototype with mc

Implementation begins by provisioning secure locker kiosks equipped with a camera, smart-card/NFC reader, keypad, and lock actuator, all controlled by an edge computer (e.g., Raspberry Pi or industrial edge module). A secure boot and encrypted filesystem protect local data. The kiosk software captures a live image when an access attempt is initiated, performs basic preprocessing and liveness checks, and packages an authentication request (card ID, PIN hash, image-template or encrypted descriptor) that is transmitted over TLS to the cloud authentication service. The cloud executes the recognition match against the enrolled profile, logs the event to an append-only encrypted audit store, and responds with an access grant or denial. From fig. 6.1 on successful approval, the kiosk actuates the lock and displays a confirmation; on failure, it triggers alerts to branch security and records CCTV/auxiliary camera footage for review. Administrative interfaces run on a secure web portal that enforces role-based access control and allows staff to review image-linked logs, perform identity re-verification, and schedule maintenance. Security measures include mutual TLS, HSM-backed key management for cryptographic operations, template hashing to avoid storing raw biometric images, periodic firmware signing checks, and privacy controls that retain raw images only under defined policies (e.g., retention for a short period or only on exception). The system is tested for latency, recognition accuracy, false accept/reject rates, and resilience to network outages via offline fallback policies.

VII. CONCLUSION

Integrating image identification and IoT into bank locker systems substantially strengthens security and auditability while improving operational efficiency. The proposed architecture combines multi-factor authentication, edge-based liveness checks, secure cloud logging, and real-time alerts to mitigate common vulnerabilities of traditional locker systems. By using privacy-preserving template storage, secure communications, and strong administrative controls, the design balances security requirements with regulatory and customer privacy needs. The solution enhances customer trust, simplifies incident investigations, and modernizes locker

management for contemporary banking operations.

VIII. FUTURE SCOPE

The **Bank Safety Locker System with Image Identification using IoT** holds significant potential for future enhancement and real-world application. In the coming years, the system can be further improved by integrating **advanced biometric authentication methods**, such as facial recognition with AI-based emotion detection and multi-factor verification using fingerprints, retina scans, or voice recognition to enhance security. Incorporating **blockchain technology** could ensure tamper-proof transaction and access logs, providing transparent and immutable security records for every locker access event. Additionally, the integration of **machine learning algorithms** could enable the system to identify unusual access patterns and generate real-time alerts for suspicious activities.

With the rise of **cloud computing**, data storage and monitoring can be made more scalable and accessible, allowing authorized personnel to access security data remotely while maintaining high levels of encryption. The system can also be extended to support **IoT-based smart surveillance**, where cameras automatically capture and analyze locker room activities. Future developments may also include **mobile app integration**, enabling customers to schedule locker access securely and receive real-time notifications of locker activities. Overall, these advancements will make the IoT-based bank locker system more intelligent, reliable, and adaptive to evolving security challenges, establishing a robust foundation for next-generation financial safety infrastructure.

IX. REFERENCES

[1]Bhargava R, Amulya H C, Jyothi K P, Keerthana R, "Smart Authentication and Secured Engine Unlocking System for Automobiles", International Journal of Scientific Research in Science and Technology , pp.653, 2021.

[2]A. Kumar, P. Sood and U. Gupta, "Internet of Things (IoT) for Bank Locker Security System," 2020 6th International Conference on Signal Processing and communication (ICSC), 2020, pp. 315-318, doi: 10.1109/ICSC48311.2020.9182713

[3]A. Chikara, P. Choudekar, Ruchira and D. Asija, "Smart Bank Locker Using Fingerprint Scanning and Image Processing," 2020 6th International Conference on Advanced Computing and Communication systems(ICACCS), 2020, pp. 725-728, doi: 10.1109/ICACCS48705.2020.9074

[4]Smart Locker: IOT based Intelligent Locker with Password Protection and Face Detection Approach. International Journal of Wireless and Microwave Technologies, MAY 2019.

[5]A. Pawar and V. M. Umale, "Internet of Things Based Home Security Using Raspberry Pi," 2018 Fourth International Conference on Computing Communication Control (ICCUBEA), 2018, pp. 1-6 doi: 10.1109/ICCUBEA.2018.869734.

[6]S. Dutta, N. Pandey and S. K. Khatri, "Microcontroller Based Bank Locker Security System Using IRIS Scanner and Vein Scanner," 2018 International Conference on Inventive Research in Computing Applications(ICIRCA),2018, pp. 53-57, doi: 10.1109/ICIRCA.2018.8597215.